

AN ELEMENTARY APPROACH TO CHARACTER SUMS OVER MULTIPLICATIVE SUBGROUPS

KE GONG

ABSTRACT. Let p be an odd prime. Using I. M. Vinogradov's bilinear estimate, we present an elementary approach to estimate nontrivially the character sum

$$\sum_{x \in H} \chi(x + a), \quad a \in \mathbb{F}_p^*,$$

where $H < \mathbb{F}_p^*$ is a multiplicative subgroup in finite prime field \mathbb{F}_p . Some interesting mean-value estimates are also provided.

1. Introduction

Let p be an odd prime, and $H < \mathbb{F}_p^*$ be a multiplicative subgroup of the finite prime field \mathbb{F}_p . After his opening work on extremely short exponential sums $\sum_{x \in H} \psi(ax)$ with ψ being the additive character of \mathbb{F}_p , Jean Bourgain posed the following problem concerning multiplicative character sums over shifted subgroup, see [C, Problem 5].

Problem 1 (J. Bourgain). *Obtain nontrivial bound on $\sum_{x \in H} \chi(x + a)$ for $H < \mathbb{F}_p^*$, $|H| \sim \sqrt{p}$, and $a \in \mathbb{F}_p^*$.*

Using I. M. Vinogradov's bilinear estimate for character sums, we shall present an elementary approach to Bourgain's character sum.

2010 *Mathematics Subject Classification*. Primary 11L40; Secondary 11N69.

Keywords. Character sums, multiplicative subgroups, bilinear estimate, finite field.

This work was supported by the Natural Science Foundation of China (Grant No. 11126150), the Natural Science Foundation of the Education Department of Henan Province (Grant No. 2011A110003), and a Québec Merit Scholarship (2011–2012).

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ -TEX

Theorem 2. *For any $H < \mathbb{F}_p^*$, we have*

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in H} \chi(x + a) \right| < p^{1/2}.$$

Thus, for any $\varepsilon > 0$ and $H < \mathbb{F}_p^*$ with $|H| > p^{1/2+\varepsilon}$, we have

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in H} \chi(x + a) \right| < p^{-\varepsilon} |H|.$$

We also obtain two mean-value estimates which suggest that an estimate for extremely short character sums may exist.

2. Vinogradov Lemma

We recall that, first in 1930s (see [V43]) and then in his monograph [V76, Russian, p. 88; English, pp. 360–361], I. M. Vinogradov obtained the following bilinear estimate (up to a $\sqrt{2}$ -factor in the upper bound) for character sums, which played a fundamental role in his studies on character sums over shifted primes.

Lemma 3 (I. M. Vinogradov). *Let p be an odd prime, $\gcd(a, p) = 1$, $\chi \neq \chi_0 \pmod{p}$,*

$$S = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x) \eta(y) \chi(xy + a),$$

$$S' = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x) \eta(y) \chi(xy(xy + a)).$$

For any complex-valued functions ξ and η with

$$\sum_{x=0}^{p-1} |\xi(x)|^2 \leq X, \quad \sum_{y=0}^{p-1} |\eta(y)|^2 \leq Y,$$

we have

$$|S| \leq \sqrt{pXY}, \quad |S'| \leq \sqrt{pXY}.$$

We present here, for the sake of completeness, the proof due to Vinogradov [V81, Chap. V, Exercise 8, **c**], where the Legendre symbol case was treated. Indeed,

Lemma 3 is a counterpart of Vinogradov's bilinear estimate for exponential sums, see [V81, Chap. VI, Exercise 8, α]).

Proof. It suffices to prove the first statement, since the second one is immediately if we take $\xi'(x) = \xi(x)\chi(x)$ and $\eta'(y) = \eta(y)\chi(y)$ as the weights.

Since

$$\begin{aligned} |S|^2 &\leq \left(\sum_{x=0}^{p-1} |\xi(x)| \cdot \left| \sum_{y=0}^{p-1} \eta(y)\chi(xy+a) \right| \right)^2 \\ &\leq X \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \sum_{y_1=0}^{p-1} \eta(y)\overline{\eta(y_1)}\chi(xy+a)\overline{\chi(xy_1+a)} \\ &= X \sum_{y=0}^{p-1} \sum_{y_1=0}^{p-1} \eta(y)\overline{\eta(y_1)} S_{y,y_1}, \end{aligned}$$

where

$$S_{y,y_1} = \sum_{x=0}^{p-1} \chi(xy+a)\overline{\chi(xy_1+a)}.$$

Thus

$$S_{y,y_1} = \begin{cases} p, & \text{if } y = y_1 = 0; \\ 0, & \text{only one of } y \text{ and } y_1 \text{ equals } 0; \\ p-1, & \text{if } y = y_1 > 0; \\ -\chi\left(\frac{y}{y_1}\right), & \text{otherwise.} \end{cases}$$

The last equality is because

$$\begin{aligned} S_{y,y_1} &= \sum_{z=0}^{p-1} \chi\left(\frac{y}{y_1}z + a\left(1 - \frac{y}{y_1}\right)\right) \overline{\chi(z)} \\ &= \chi\left(\frac{y}{y_1}\right) \sum_{z=1}^{p-1} \chi(z)\overline{\chi(z)} \chi\left(1 + a\frac{y_1}{y}\left(1 - \frac{y}{y_1}\right)z^*\right) = -\chi\left(\frac{y}{y_1}\right) \end{aligned}$$

by taking $xy_1 + a \equiv z \pmod{p}$. Therefore

$$\begin{aligned}
|S|^2 &\leq X \left(p|\eta(0)|^2 + (p-1) \sum_{y=1}^{p-1} \eta(y) \overline{\eta(y)} - \sum_{\substack{y=1 \\ y \neq y_1}}^{p-1} \sum_{y_1=1}^{p-1} \eta(y) \overline{\eta(y_1)} \chi\left(\frac{y}{y_1}\right) \right) \\
&= X \left(p|\eta(0)|^2 + p \sum_{y=1}^{p-1} \eta(y) \overline{\eta(y)} - \sum_{y=1}^{p-1} \eta(y) \overline{\eta(y)} - \sum_{\substack{y=1 \\ y \neq y_1}}^{p-1} \sum_{y_1=1}^{p-1} \eta(y) \overline{\eta(y_1)} \chi\left(\frac{y}{y_1}\right) \right) \\
&= X \left(p \sum_{y=0}^{p-1} \eta(y) \overline{\eta(y)} - \sum_{y=1}^{p-1} \sum_{y_1=1}^{p-1} \eta(y) \overline{\eta(y_1)} \chi\left(\frac{y}{y_1}\right) \right) \\
&= X \left(p \sum_{y=0}^{p-1} |\eta(y)|^2 - \left| \sum_{y=1}^{p-1} \eta(y) \chi(y) \right|^2 \right) \leq pXY,
\end{aligned}$$

which completes the proof. \square

2. Proof of Theorem 2

Here and below, we denote $A(\cdot)$ the indicator function for a subset A of \mathbb{F}_p .

Indeed, once taking η to be the indicator function of multiplicative subgroup $H < \mathbb{F}_p^*$ in the proof of Lemma 3, we have

$$|S|^2 \leq |H| \left(p|H| - \left| \sum_{x \in H < \mathbb{F}_p^*} \chi(x) \right|^2 \right).$$

But we only need a weak upper bound for our use below.

Recall that $a \in \mathbb{F}_p^*$. We first write

$$\sum_{x \in H} \chi(x + a) = \frac{1}{|H|} \sum_{x, y \in H} \chi(xy + a) = \frac{1}{|H|} \sum_x \sum_y H(x) H(y) \chi(xy + a),$$

then apply Lemma 1 directly to obtain

$$\left| \sum_{x \in H} \chi(x + a) \right| \leq \frac{1}{|H|} \sqrt{p|H| \cdot |H|} = \sqrt{p}. \quad (1)$$

3. Mean-value estimate, I

We find that the following identity could be obtained from generalizing the classical results due to Vinogradov [V81, Chap. VII, Exercise 1], Davenport and Erdős [DE, Lemma 1].

Theorem 4. *For any subset $D \subset \mathbb{F}_p^*$, we have the identity*

$$\sum_{a \in \mathbb{F}_p} \left| \sum_{x \in D} \chi(x+a) \right|^2 = p|D| - |D|^2. \quad (2)$$

Proof. Indeed,

$$\begin{aligned} \sum_{a \in \mathbb{F}_p} \left| \sum_{x \in D} \chi(x+a) \right|^2 &= \sum_{a \in \mathbb{F}_p} \sum_{x, y \in D} \chi(x+a) \overline{\chi}(y+a) \\ &= \sum_{a \in \mathbb{F}_p} \sum_{x \in D} |\chi(x+a)|^2 + \sum_{\substack{x, y \in D \\ x \neq y}} \sum_{a \in \mathbb{F}_p} \chi(x+a) \overline{\chi}(y+a) \\ &= (p-1)|D| - |D|(|D|-1) \\ &= p|D| - |D|^2. \end{aligned}$$

Note that the second to last equality is due to the fact

$$\sum_{a \in \mathbb{F}_p} \chi(x+a) \overline{\chi}(y+a) = -1,$$

which is a consequence of the observation that the congruence

$$x+a \equiv z(y+a) \pmod{p}$$

establishes a one-to-one correspondence between all a with $a \not\equiv -y$ and all z with $z \not\equiv 1$. \square

We remark that, (2) could be compared with its counterpart for exponential sums (see Konyagin [K, Lemma 2]). That is, for any subset $D \subset \mathbb{Z}_q$ (q is a positive integer), there holds

$$\sum_{a \in \mathbb{Z}_q \setminus \{0\}} \left| \sum_{x \in D} e_q(ax) \right|^2 = |D|(q - |D|).$$

4. Mean-value estimate, II

In this section we present another different type mean-value estimate. For $a \in \mathbb{F}_p^*$, we have

$$\frac{1}{p-1} \sum_{\chi \pmod{p}} \left| \sum_{n \in H} \chi(n+a) \right| \leq \sqrt{|H|}.$$

Proof. Indeed,

$$\begin{aligned} \left(\sum_{\chi \pmod{p}} \left| \sum_{n \in H} \chi(n+a) \right| \right)^2 &\leq (p-1) \sum_{m \in H} \sum_{n \in H} \sum_{\chi \pmod{p}} \chi \left(\frac{m+a}{n+a} \right) \\ &\leq (p-1)((p-1)|H| + 0) \\ &= (p-1)^2 |H|, \end{aligned}$$

which completes the proof. \square

If $a = 0$, we recall that Shkredov [S, p. 607] has obtained $\sum_{\chi} |\sum_{n \in H} \chi(n)| \leq p$. Indeed, we can even obtain an identity. Here we present a proof due to A. Granville.

If H is the subgroup of order $(p-1)/k$, then

$$H(n) = \frac{1}{k} \sum_{\psi: \psi^k = \chi_0} \psi(n),$$

so that

$$\sum_n H(n) \chi(n) = \frac{1}{k} \sum_{\psi: \psi^k = \chi_0} \sum_n (\psi \chi)(n)$$

and this equals $\frac{p-1}{k}$ if $\chi = \overline{\psi}$ for some ψ satisfying $\psi^k = \chi_0$, and equals 0 otherwise. Hence we see that

$$\sum_{\chi} \left| \sum_{n \in H} \chi(n) \right| = \sum_{\chi} \left| \sum_n H(n) \chi(n) \right| = \sum_{\psi: \psi^k = \chi_0} \frac{p-1}{k} = p-1.$$

5. Final remarks

Firstly, estimate (1) can be obtained by Weil's estimate through expressing the indicator function of H as $H(n) = \frac{1}{k} \sum_{\psi: \psi^k = \chi_0} \psi(n)$. However, our method is completely elementary.

Secondly, using the estimate for S' in Lemma 3, we have for $a \in \mathbb{F}_p^*$

$$\left| \sum_{x \in H} \chi(x(x+a)) \right| = \frac{1}{|H|} \left| \sum_x \sum_y H(x) H(y) \chi(xy(xy+a)) \right| \leq \sqrt{p},$$

which provides for the nonlinear character sums the same upper bound as the linear case in Theorem 2.

We remark that I. E. Shparlinski has posed the following problem, which has immediate implications to polynomial factorization over finite fields.

Problem 5 (I. E. Shparlinski). *Estimate nontrivially*

$$\sum_{x \in H} \chi((x+a)(x+b)), \quad ab(a-b) \in \mathbb{F}_p^*$$

for $H < \mathbb{F}_p^*$ and $|H| \sim \sqrt{p}$.

Finally, we would like to pose the following problem, which could also be dealt directly by Weil's estimates for character sums with rational functions argument. But no elementary approach is known.

Problem 6. *Estimate nontrivially the sums*

$$\sum_{x \in H} e\left(\frac{kx + \ell x^*}{p}\right), \quad \sum_{x \in H \setminus \{-a\}} e\left(\frac{k(x+a)^*}{p}\right)$$

for $H < \mathbb{F}_p^*$ with $|H| \sim \sqrt{p}$ and $k, \ell, a \in \mathbb{F}_p^*$.

Acknowledgement

I would like to thank Professors Andrew Granville, Chaohua Jia and Igor Shparlinski for their interests and comments on this work. I am grateful to Professor Sergei Konyagin for sending his Russian paper.

REFERENCES

- [C] M.-C. Chang, *Character sums in finite fields*, Finite Fields: Theory and Applications, pp. 83–98, Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010.
- [DE] H. Davenport and P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), 252–265.
- [K] S. V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, IV International Conference “Modern Problems of Number Theory and Its Applications”: Current Problems, Part III (Tula, 2001), Mosk. Gos. Univ. im. Lomonosova, Mekh. Mat. Fak., Moscow, 2002, pp. 86–114. (Russian)
- [S] I. D. Shkredov, *On monochromatic solutions of some nonlinear equations in $\mathbb{Z}/p\mathbb{Z}$* , Math. Notes **88** (2010), 603–611.
- [V43] I. M. Vinogradov, *An improvement of the estimation of sums with primes*, Izv. Akad. Nauk SSSR Ser. Mat. **7** (1943), 17–34. (Russian)
- [V76] I. M. Vinogradov, *Special Variants of the Method of Trigonometric Sums*, Nauka, Moscow, 1976 (Russian); English transl. in his *Selected Works*, Springer-Verlag, Berlin, 1985.
- [V81] I. M. Vinogradov, *Foundations of the Theory of Numbers*, 9th ed., Nauka, Moscow, 1981. (Russian)

DEPARTMENT OF MATHEMATICS, HENAN UNIVERSITY, KAIFENG, HENAN 475004, P.R. CHINA

E-mail address: kg@henu.edu.cn